PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
H04L 12/14, 29/06

A1

(11) International Publication Number: WO 99/33224

(43) International Publication Date: 1 July 1999 (01.07.99)

(21) International Application Number: PCT/GB98/03755

(22) International Filing Date: 15 December 1998 (15.12.98)

(30) Priority Data:

97310358.3	19 December 1997 (19.12.97)	EP
9726934.4	19 December 1997 (19.12.97)	GB
98304429.8	4 June 1998 (04.06.98)	EP
9812060.3	4 June 1998 (04.06.98)	GB

(71) Applicant *(for all designated States except US)*: BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY [GB/GB]; 81 Newgate Street, London EC1A 7AJ (GB).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: FAIRMAN, Ian, Ralph [GB/GB]; 28 Camden Road, Ipswich, Suffolk IP3 8JW (GB). BRISCOE, Robert, John [GB/GB]; Home Farm, Parham, Woodbridge, Suffolk IP13 9NW (GB).

(74) Agent: WELLS, David; BT Group Legal Services, Intellectual Property Dept., Holborn Centre, 8th floor, 120 Holborn, London EC1N 2TE (GB).

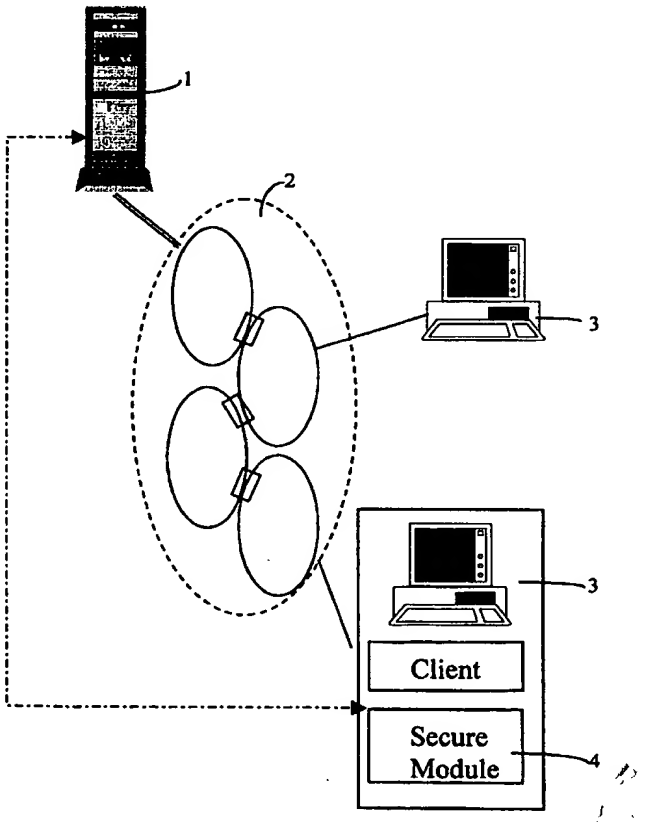
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: DATA COMMUNICATIONS

(57) Abstract

In a data communications system a remote data source outputs data as a series of application data units (ADUs). Each ADU is individually encrypted with a different key. The keys are transmitted (for example using Internet multicasting) via a communications network to one or more customer terminals. At the terminals a sequence of keys is generated for use in decrypting the ADUs. A record is kept of the keys generated, and this record may subsequently be used to generate a receipt for the data received by the customer. The keys may be generated, and the record stored within a secure module such as a smartcard.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

DATA COMMUNICATIONS

The present invention relates to a data communications system, and in particular to a system using an extensive public network such as the Internet.

Hitherto, users have typically been charged for Internet usage following a subscription model in which they pay a flat-rate fee to an Internet Services Provider (ISP) for access to the Internet and use of network resources is subsequently free of charge. The different networks and routers making up the Internet have then endeavoured to meet the need of any particular application on a "best effort" basis. It has been recognised that this method of operation is not appropriate for applications such as multimedia conferencing which use a lot of network resources, and which ideally require a guaranteed quality of service (QoS). A customer for such services may therefore pay a premium to an Internet service provider in order to receive a guaranteed QoS for a given session, or over an extended period of time. More generally, there may be a need to charge customers according to the amount of data transmitted. This might be used, for example, to provide a charging mechanism for access to on-line data sources, such as a video library.

Where the customer is paying for a certain specified quality of service, or for a certain amount of data received, there arises the problem of resolving any disputes between the customer and the service provider as to the level of service the customer has received in a given period. A customer might, for example, pay for an enhanced QoS level for a session of video conferencing. If however the network or service provider then fails to provide the required QoS, for example because a high proportion of data packets has been lost or because the video source became over-loaded, then the customer might claim a refund. However, while conventional networks, such as the PSTN, incorporate extensive and reliable billing systems which carefully record details of all calls and generate reliable records, no such billing/auditing structure exists within or across the Internet. Moreover, it would be undesirable to incorporate a conventional billing structure in the Internet or any other similar public data network, since this would add considerably to the operational costs of the network. There remains a need therefore for alternative mechanisms for resolving any disputes between parties as to the quality of service which has been delivered.

According to a first aspect of the present invention, there is provided a method of operating a data communications system comprising:

a) at a remote data source, outputting a plurality of application data units (ADUs)

b) encrypting the ADUs;

c) communicating the ADUs to a customer terminal;

d) in the locality of the customer terminal, decrypting the ADUs;

e) storing a record of the ADUs decrypted in step (d); and

f) subsequently generating a receipt for ADUs received at the customer terminal by reading record data stored in step (e) .

The present invention provides a new approach to the generation of an auditable record of the data received by a customer connected to a data communications network. The data source transmits the data as a series of ADUs. These ADUs are typically application-level entities, and need not correspond to the frame structure, if any, of the transmission layer of the network. The ADUs might correspond, for example, to successive minutes of video delivered from a video server or to individual strokes on a white board in a conferencing application. Each successive ADU is then encrypted. The ADU need not be encrypted in a single operation. It may be broken down into packets before encryption. However, the same key is used to encrypt each packet in any one ADU. In order for the customer to be able to use the data, each ADU has to be decrypted. A record is kept of the decryption of the ADUs. This record may comprise a count of the number of ADUs decrypted. This record may itself be encrypted. This then provides a verifiable record which can be used, for example, to resolve disputes as to the number of ADUs received in a given time period.

The invention includes, but is not limited to, data communications systems in which the ADU's are communicated over, e.g., a federated public data network such as the Internet. It also encompasses systems in which the step of communicating ADU's is carried out, e.g., by physically distributing a data carrier such as a CD-ROM containing the ADU's. It also encompasses both multi-cast and uni-cast data communication systems, and systems in which there is more than one data source communicating data to a particular terminal.

The invention it is also applicable in a wide range of contexts, wherever it is necessary control access, and particularly to establish proof of receipt (or of

failure to receive) data items. Possible applications include multicast audio/video streams for Video-on-Demand, network radio or surveillance; controlling access to the contents of CD ROMS or other storage media carrying software or multimedia data; controlling access to a set of vouchers giving access to other services; a multicast stream of messages such as stock prices, communications network prices, electricity prices, network management messages, news items, portfolio information, team briefings, standards documents, academic papers, magazines, product reviews, black lists, criminal intelligence, legal precedents, property profiles, pharmaceutical test results etc; a sequence of multicast messages within a network game, virtual world or simulation scenario (e.g. an aptitude exam), possibly just those messages that control access, but also possibly any data messages for which proof of reception is crucial to the fairness of the result of the simulation.

The invention may also be applied in a community of interest network (COIN) or a virtual private network (VPN), as further described below.

As exemplified in the detailed embodiment below, different keys may be used for encryption and decryption of different ADUs. The keys are generated in such a way that it is not practically possible for the customer to predict a key value from previous keys. The record of the decryption of the ADUs may then be derived by storing a count of the number of keys generated at the customer terminal. Other data may also be stored, such as the time of the session and/or the time at which each key is generated.

The customer terminal may be a personal computer or any other appropriate device, such as, for example, a Java-enabled mobile cellular telephone.

Preferably the steps of generating a record (and optionally of generating a plurality of different keys) are carried out by a secure module located at the customer terminal. The secure module provides a region in the customer terminal which is effectively under the control of the data provider, and which is not readily accessible to the customer. The use of such a secure module further enhances the reliability of the stored record. The secure module may be a software module which executes a cryptographic algorithm. This might be implemented, for example, as a Java program distributed by the operator of the remote data source as part of the process of setting up a session. To provide still higher levels of security, it is preferred that the secure module should include a dedicated

processor and store located within a tamper-proof unit. Examples of such secure modules include smartcard structures, and cryptographic PC cards.

When the secure module has only a relatively low processing power, as may be the case, for example, when it is a smartcard, then preferably that module is required simply to output the different respective keys. Other processes running in the main part of the customer terminal are then responsible for decrypting the ADUs. Alternatively, when the secure module has more processing power, as when, for example, a cryptographic co-processor card is used, then preferably the encrypted ADUs are passed to the secure module and the module generates a key, decrypts the ADUs, and passes the decrypted ADUs out, for example, to an application programme running on the customer terminal. In this case it is not necessary to generate a new key for each ADU since the key is kept within the secure module.

Preferably the remote data source generates and transmits to the customer terminal a seed value, and the plurality of different keys are generated from the said seed value. A fresh seed value may be used for each session.

The ADUs from the remote data source may be multicast to a plurality of different customer terminals. In this case preferably seed values for the generation of the plurality of different keys are distributed to the plurality of terminals.

Preferably a digital watermark, that is a characteristic variation in the data, is added to the ADUs. This variation may be generated directly in or subsequently to the said step of decrypting the ADUs or a watermarked key may be supplied to decrypt the ADU. In this latter case, the characteristic variation in the key automatically results in a traceable variation in the data decrypted using the key.Digital watermarking is a well-known technique whereby, for example, insignificant bits of a digital data stream may be varied in a characteristic fashion traceable separately to each party receiving the data. If the data is then copied and passed on, the secondary source can be identified by inspecting the insignificant bits. The use of digital watermarking is particularly valuable in the context of the present invention, since it facilitates detection of attempts to undermine the security of the system by collusion between two or more customers, for example by one customer decrypting and retransmitting ADUs.

According to a second aspect of the present invention, there is provided a data communication system comprising:

a) a remote data source arranged to output a plurality of ADUs;

b) encryption means for encrypting a plurality of ADUs with different respective keys;

c) a communications network connected to the encryption means;

d) a customer terminal connected to the communications network and arranged to receive encrypted ADUs via the communications network;

e) key generation means located in the locality of the customer terminal and arranged to generate a plurality of different keys for decrypting different respective ADUs; and

f) a store at the customer terminal for storing a record of keys generated by the decryption means.

Preferably the record in the store is authenticated, for example, using a cryptographic signature.

According to another aspect of the present invention, there is provided a method of operating a data communications system comprising:

a) at a remote data source, outputting a plurality of ADUs;

b) encrypting different ones of the plurality of ADUs using different respective keys;

c) communicating the ADUs to a customer terminal;

d) in the locality of the customer terminal, generating a plurality of different keys for decrypting different respective ADUs received at the customer terminal; and

e) storing a record of the keys generated.

According to a further aspect of the present invention there is provided a method of operating a data communications system comprising:

a) at a remote data source, outputting a plurality of application data units (ADUs) ;

b) encrypting the ADUs;

c) communicating the ADUs to a plurality of customer terminals;

d) in the locality of each customer terminal, decrypting the ADUs; and

e) inducing a different characteristic variation in the value of the ADU's at different respective terminals.

The use of digital watermarks in decrypted ADU can advantageously be used also in otherwise conventional systems, including systems in which no

receipt is generated.

The invention also encompasses customer terminals and data servers adapated for implementing the invention in any of its aspects.

Methods and apparatus embodying the present invention will now be described in further detail, by way of example only, with reference to the accompanying drawings in which;

Figure 1 is a schematic of a data communication system embodying the network;

Figure 2 is a schematic showing in further detail the functional components of the customer terminal in the system of Figure 1;

Figure 3 is a flow diagram showing the principal phases of operation of the system of Figure 1;

Figure 4 is a flow diagram showing in further detail the verification phase;

Figure 5 is a flow diagram showing in further detail the initialisation phase;

Figure 6 is a flow diagram showing in further detail the received/decrypt phase;

Figure 7 is a flow diagram showing in further detail the receipt phase;

Figure 8 shows an alternative embodiment;

Figure 9 shows a software architecture for a customer terminal.

A data communications system includes a data server 1 connected via a data communications network 2 to a number of customer terminal 3. Although for ease of illustration only two customer terminals are shown, in practice the data server 1 may communicate simultaneously with many terminals. In the present example, the data communications network 2 is the public Internet and is formed from a number of sub-networks 2a-2d. The sub-networks and the associated routers support IP (Internet Protocol) multicasting.

In the present example, the data server 1 is a video server. The data server reads a video data stream from a mass storage device and compresses the data using an appropriate compression algorithm such as MPEG 2. An encryption module in the data server 1 then divides the compressed video data stream into ADUs. For example each ADU may comprise data corresponding to one minute of the video signal. An encryption algorithm then encrypts the ADUs. Suitable encryption algorithms include DES (Data Encryption Standard) (US Federal Standard FIPS PUB46). This is a conventional private key algorithm. A common

encryption algorithm is used for all of the ADUs in one session. In this embodiment, a sequence of keys is used, with a different key for each successive ADU. (The ADU referred to in this embodiment is an application-level entity created for the purposes of encryption and is to be distinguished from conventional video "frames").

At each customer terminal, incoming ADUs are processed with the aid of a secure module 4. As described in further detail below, the secure module 4 generates a sequence of keys corresponding to those used originally to encrypt the ADUs. The keys may be passed out to the main processor of the customer terminal to allow the data to be decrypted. Alternatively, the secure module itself may carry out the step of decryption. In either case, the secure module stores a record of the decryption of the ADUs. This record may comprise, for example, a count of the total number of keys issued in the course of a session and hence of the number of ADUs decrypted, together with a session ID and a record of the time of the session. Any ADUs arriving too late or corrupted may be discarded without decryption or without requesting a key to decrypt them.

Prior to commencing a session, a customer terminal 3 may have contracted with the operator of the data network 2 for a quality of service (QoS) which requires a specified minimum number of ADUs to be delivered per unit time. If subsequently, congestion in the network 2 causes the rate of ADU delivery to fall below that specified in the contract, then the customer terminal 3 request from the data server 1 a refund of charges for the session. To validate this request, the data server 1 requests from the secure module 4 a "receipt". This receipt includes the data recorded in the data store and so provides a tamper-proof indication of the number of ADUs decrypted and made available to the customer in the course of a specified session. In general, this receipt will only be trusted by the party encrypting the data, not a party such as the network operator simply transmitting data encrypted without its knowledge. However, the encryption software used by the data source may be certified by a third party trusted by both the network provider and the data source. If the decryption software is also certified by this trusted third party as described below, it may then sign the receipt on behalf of the trusted third party so that the network operator can trust it.

Figure 2 shows the principal functional components of the customer terminal relevant to the present invention. A network interface 22 communicates

ADUs to and from the data network. The ADUs pass from the interface 22 to a secure module 23. The secure module 23 has sub-modules comprising a decryption module D a key generation module K and a secure store S. The key generation module passes a series of keys to the decryption module which decrypts a series of ADUs received from the interface 22 and passes these to an application layer module 24. This carries out further processing and passes the resulting data to an output device, which in this example is a video display unit VDU 25. In a preferred implementation, the interface 22 may be embodied in hardware by an ISDN modem and in software by a TCP-IP stack. The secure module 23 may be, for example, a smartcard which is interfaced to the customer terminal via a PCMCIA socket. Suitable smartcards are available commercially from Gemplus and other companies. The smartcard may use one of a number of standard data interfaces such as the Java card API (application programmer's interface) of Sun Microsystems, or the Microsoft smartcard architecture. Alternatively, the secure module may be embodied by a PCI cryptographic co-processor card such as that available commercially from IBM.

Figure 9 illustrates a software architecture for the customer terminal. The application layer on the terminal is supported by a decrypting data channel which in turn overlies a data channel layer connected e.g. to a network. The decrypting data channel has associated with a decrypter module. This decrypter module calls resources in a secure module (shown within dashed box) comprising a receipting key generator a key generator, and a receipt store. It will be understood that this architecture is given by way of example only, and alternatives are possible within the scope of the invention. For example, the receipt store may be outside the secure module.

Figure 3 shows the main phases in the operation of the system described above. In phase P1, the server verifies that the secure module in the customer terminal is trustworthy and has a recognised identity. In phase P2 the secure module is initialised to decode data for a particular session. In phase P3 the data is transmitted and decryption carried out and in stage P4, which is optional, a receipt is generated. These phases will now be described in further detail.

When the secure module is, for example, a smartcard, then that smartcard is issued by the manufacturer with a unique public/private key pair. This key pair may be certified by a trusted third party. In phase P1, the server carries out steps

to confirm that the smartcard does indeed come from a trusted supplier. The steps of phase P1 are shown in figure 4. In step S1 the server generates a random string. In step S2, the server sends the random string via the data network to the customer terminal. In step S3, the random data string is passed to the secure module (e.g. the smartcard). In step S4 the smartcard signs the random string with its private key. In step S5 the smartcard returns the signed string together with its relevant public key (which has itself been signed by the trusted third party) to the client application running on the customer terminal. In step S6, that client application returns the signed string and the signed public key via the data communications network to the server. In step S7 the server verifies the signed random string.

As shown in Figure 5, to set up the secure module to decode data in a particular session, the server first generates (s51) a seed value for use with an appropriate pseudo-random or chaotic function to generate a series of keys. It also generates a session key (s52). The server encrypts the seed value using the secure module's public key (s3). It then transmits the encrypted seed value and the session key to the customer terminal (s54). The client application passes the encrypted seed value and session key on to the secure module (s55). The secure module decrypts the seed value and session key with its private key. The secure module sets an ADU counter to zero (s56) and initialises a sequence generator with the seed value (s57). The customer terminal is then ready to receive and decrypt ADUs.

The server subsequently sends a series of ADUs to the client. Each ADU has an ADU number. Each ADU might also have a session key transmitted with it. The sequence of steps for the nth ADU is illustrated in Figure 6. In step s61 the server sends the encrypted nth ADU to the client. The client requests the key x for ADU n from the secure module (s62). The secure module records the request (s63). The smartcard then returns the key x to the client (s64). The client deciphers the ADU using x (s65). The client tests to determine whether the ADU is the last of a session (s66). If not then the steps are iterated for the n + 1th and subsequent ADUs.

In the step of recording the request (s63) referred to above, the record of the request may simply be stored as a single incrementing counter. However, some stringent scenarios may require audit trails where each detailed record of receipt is

stored. If the list of records becomes too large to be stored on the smartcard, it can be hashed and the hash and the time can then be signed using the smartcard's private key, the record, hash and signature then being passed to the client for storage. Subsequently, if further records again become too large, the hash of the previous records can be retrieved from the client by the smartcard, and, having checked the signature of the previous hash is valid, the hash can be prepended to the new records, a new hash generated from the combined new records and old hash, then the new records and new hash can be appended to the old records on the client followed by the digital signature of the new hash. The length of each chunk of hashed records would have to be known by the data source in order to check the signature on the receipt. This may be by a convention, or by including it in a header to the receipt.

In setting up the session, the customer has previously negotiated an agreement with the service provider as to the QoS level for the session. For an application such as video on demand this level may be stringent: for example the customer may require that no application-level ADU is lost in transmission. If a ADU arrives too late at the client, it can can be discarded and is effectively considered to have been lost. If then this QoS level is not met, then the customer requests a refund from the service provider. The request for refund might specify, for example, that there was ADU loss at a specified time into the video transmission. In processing such a request, the server requires a receipt from the customer. As shown in Figure 7, in step s71 the client requests a receipt for a specified session s from the secure module. The secure module reads the data which it recorded for that session and generates a receipt containing that data (s72). The secure module signs the receipt with the secure module's private key (s73). The secure module returns the signed receipt to the client (s74). Alternatively, the secure module may have already signed and stored its receipts on the client terminal if it was short of storage space as described above. When next adding to the data forming the receipt on the client, the secure module The client in turn transmits the signed receipt to the server (s75). The server checks the signature on the receipt using the public key of the secure module (s76). The public key may be read from a database stored at the server. Having verified the signature, the server can then check the customers claim for a refund using the data contained in the receipt. This data may show, for example, a discrepancy

between the number of ADUs decrypted in a session and the number transmitted by the server, thereby substantiating the customer's claim that a ADU was lost.

As noted in the introduction above, the ADU's may be decrypted in such a way that at each one of a number of customer terminals a different characteristic variation is present in the data. This variation may be generated directly in the said step of decrypting the ADUs or a watermarked key may be supplied to decrypt the ADU. In this latter case, the characteristic variation in the key automatically results in a traceable variation in the data decrypted using the key. The use of watermarked keys is described, for example, in Ross Anderson, "Chameleon - A New Kind of Stream Cipher Encryption" in Haifa in January 1997. <http://www.cl.cam.ac.uk/ftp/users/rja14/chameleon.ps.gz>

Where digital watermarks are used, the operator of the data server, or some other interested party, may subsequently use the watermark, for example, to identify the secondary source of data copied and forwarded by one customer terminal to another. Given a sample of the data, the data server then inspects the data and compares the characterstic variations with data stored on the server that correlates the variations with respective customer terminals. Similarly the watermark may be used to detect collusion where one customer forwards keys for ADU decryption to another.

While in the examples so-far described, the ADU's are communicated over a network, in an alternative embodiment distribution is effected using a data carrier such as CD-ROM or some other portable storage medium. In this case the set up of the secure module on a smart card at the customer location is carried out as before - over the Internet. The data on the distribution medium is separated into ADUs, each with a sequence number and each encrypted with different keys as before. During reading of the data from the CD etc. the smart card generate keys, which could all be achieved off-line. However, the request for a receipt and the response are carried out on-line via the Internet or other appropriate communications network as before.

The examples described above may be used in the context of a community of interest network (COIN) or a virtual private network (VPN). In this case each source of information would split its data into ADUs and transmit each ADU encrypted with different keys across the COIN. The same ADU would always be transmitted with under the same key no matter how many times it was transmitted to different parties within the COIN. Sources of information might be direct, such as the parties involved in

the COIN or indirect such as Web servers or caches commonly accessible to all parties within the COIN. In the indirect case, the information would be sent to the Web server or cache with its sequence number in the clear but data encrypted. It would be stored in the same encrypted form as it had been first transmitted. Only when the final recipient accessed the Web server or cache would their smart card generate the key for decryption and record receipt of the information. The watermarking techniques described previously could be used if tracing of who was passing on decrypted data was required.

Figure 8 shows a further alternative embodiment, in which multiple data sources 1,1a communicate data to the customer terminals. Although, for ease of illustration, only two data sources are shown, in practice the system may include many more sources. Where multiple sources are generating data, it is possible to use the invention on a per-source basis, with each receiver entering into the setup phase with each source. However, for large numbers of sources, this becomes unscalable and time-consuming. Instead, in a preferred implementation, a sequence id of any ADU arriving at any receiver consists of two parts, the sender id and the per-sender sequenceid. The sender id may be its IP address and port number, in which case these would already be in the header of each packet. The sender id acts as an offset to the primary seed to produce a secondary seed (e.g. by XORing it with the seed). Thus each smart card operates as many key sequences as it hears senders, each sequence effectively seeded from the same primary seed, but then offset to a secondary seed before starting each sequence in a similar way to the pseudo-random or chaotic seqences described below.

Whenever an ADU arrives, the sender id is examined to look-up the correct sequence, then the sequence id allows the correct key to be generated. This allows each receiver to only pass through the set up once for all senders in a multi-sender session.

The session initiator generates the primary seed and passes it to each sender using regular cryptograpic privacy (e.g. under the public key of each sender). Each sender offsets the primary seed with their own id to produce their secondary seed, which they would use to start the key sequence for ADUs they sent.

Any sender may take any receiver through the setup phase by passing it the primary seed, assuming there is some way for any sender to establish who was an authorised receiver (e.g. a list supplied and signed by the session initiator, or a token

the initiator gave to each receiver in return for payment, which each receiver had to reveal to any sender).

The sequence used for generating the keys in the above examples may be distributed to customers terminals using HTTP (hypertext transfer protocol) as Java code. A suitable chaotic function is:

$$x_{n+1} = 4rx_n(1-x_n)$$

When $r = 1$ this function takes and generates numbers in the range 0 to 1. A chaotic function such as this has the property that any errors in the value of xn grow exponentially as the function is iterated. In use, the secure module uses a higher accuracy internally than the accuracy of the key values exposed to the client. For example the secure module may use 128-bit numbers internally and then only return to the client the most significant 32 bits. In generating the key values, the chaotic function is iterated until the error in the value returned to the client grows bigger than the range. This then prevents the user guessing the sequence from the values returned by the secure module.

As an alternative or additional security measure, a different function may be used for each session. This serves to further reduce the possibility of the customer predicting sequence values.

Table 1 below list Java code for implementing a chaotic function. It returns the next number in a sequence, or the nth number in a sequence.

The key values need not necessarily be generated by a sequence. Instead other functions of the form k=f(seed, ADU i.d.), where k is a key value, may be used. For example, the binary values of the ADU identity might be used to select which of a pair of functions is used to operate on the seed value. Preferably a pair of computationally symmetric functions are used. For example , right or left-shifted XOR (exclusive OR) operations might be selected depending on whether a binary value is 1 or 0. If we label these functions A and B respectively, then, e.g., ADU number six , i.e. 110, has a key generated by successive operations AAB on the seed value.

Related inventions are described in the applicant's co-pending international application filed this day, entitled "data communications", (Applicant's reference A25728). The contents of that co-pending application are incorporated herein by reference.

```
/** Class to implement a chaotic sequence */

public class SecureSequence {

  protected int seqNum;
  protected double currNum;


  /** Create a SecureSequence object from a new seed */

  public SecureSequence (double currNum) {
    seqNum = 0;
    this.currNum = currNum;
  }


  /** Return the next number in the sequence */

  public int next() {
    ++seqNum;

    for (int i = 0; i < 20; ++i)  // 20 iterations is a guess,
could use less
      currNum = 4 * currNum * (1 - currNum);

    // return the most significant 32 bits of a 64 bit number

    return (int)((double)Integer.MAX_VALUE * currNum);

  }


  /** Return the current sequence number of the last number
returned */
```

```
    public int sequenceNumber() {
      return seqNum;
    }


  /** Return the number in the sequence at the requested
position in
      the sequence */

    public int next(int seqNum) {

      // if the number is too small return zero (should really be
an exception)

      if (seqNum <= this.seqNum)
        return 0;

      // iterate through the sequence to get to the right number

      while (this.seqNum != seqNum)
        int value = next();

      return value;0
    }
}
```

CLAIMS

1. A method of operating a data communications system comprising:

a) at a remote data source, outputting a plurality of application data units (ADUs);

b) encrypting the ADUs;

c) communicating the ADUs to a customer terminal;

d) in the locality of the customer terminal, decrypting the ADUs;

e) storing a record of the ADUs decrypted in step (d); and

f) subsequently generating a receipt for ADUs received at the customer terminal by reading record data stored in step (e) .

2. A method according to claim 1, in which the record stored in step (e) is generated by a secure module located at the customer terminal.

3. A method according to claim 2, in which the secure module encrypts the record and outputs it for storage outside the secure module

4. A method according to claim 2 or 3 in which the encrypted ADUs are passed to the secure module, and the secure module outputs decrypted ADUs.

5. A method according to any one of the preceding claims, in which each of a plurality of ADUs output by the data source is encrypted with a different key, and a plurality of corresponding keys are generated at the customer terminal.

6. A method according to claim 5 when dependent on any one of claims 1 to 3, in which the secure module outputs the plurality of corresponding keys and the customer terminal uses the said keys to decrypt the plurality of ADUs.

7. A method according to claim 5 or 6, in which the remote data source generates and communicates to the customer terminal a seed value and the plurality of different keys are generated from the said seed value.

8 A method according to any one of the preceding claims, including applying different characteristic variations to data decrypted at different respective customer terminals.

9. A method according to claim 8, in which the characteristic variation is applied after decryption of the data by a secure module.

10. A method according to claim 8, including generating a key for decryption of data, which key includes a characteristic variation, and the said characteristic variation in the in the data is induced by the characteristic variation in the key.

11. A method according to any one of the preceding claims including returning the receipt to the server .

12. A data communications system comprising

a) a remote data source arranged to output a plurality of ADUs;

b) encryption means for encrypting the plurality of ADUs;

c) a communications network connected to the encryption means.

d) a customer terminal connected to the communications network and arranged to receive encrypted ADUs via the communications network;

e) decryption means located in the locality of the customer terminal and arranged to decrypt the ADUs received at the customer terminal from the communications network;

f) a store at the customer terminal for storing a record of ADUs decrypted by the decryption means;

g) means for reading record data from the store and generating thereby a receipt for ADUs received and decrypted by the customer terminal.

13. A data communications system according to claim 12, in which the communications network is a packet-switched network.

14. A data communications system according to claim 12 or 13, in which a secure module in the customer terminal is arranged to generate the said record.

15. A data communications system according to claim 14, in which the secure module is arranged to encrypt the record

16. A data communications system according to claim 14 or 15, in which the encryption means are arranged to encrypt different ADUs with different respective keys, and the secure module is arranged to generate a plurality of keys for decrypting the plurality of ADUs received at the customer terminal.

17. A customer terminal for use in a method according to any one of claims 1 to 11, the customer terminal comprising:

a) a data interface for receiving data from a data communications medium;

b) decryption means connected to the data interface and arranged to decrypt ADUs received via the data interface;

c) means for generating a record of ADUs decrypted by the decryption means; and

d) means for reading record data and generating thereby a receipt for ADUs received and decrypted by the decryption means.

18. A customer terminal according to claim 17, in which the means for generating a record is a secure module.

19. A customer terminal according to claim 16, in which the secure module is arranged to encrypt the record.

20. A customer terminal according to claim 18 or 19 in which the secure module is arranged to generate a plurality of keys for decrypting the plurality of ADUs received at the customer terminal.

21. A method of operating a data communications system comprising:

a) at a remote data source, outputting a plurality of ADUs

b) encrypting different ones of the plurality of ADUs using different respective keys;

c) communicating ADUs to a customer terminal;

d) in the locality of the customer terminal, generating a plurality of different keys for decrypting different respective ADUs received at the customer terminal;

e) storing a record of the keys generated.

22. A data communications system comprising

a) a remote data source arranged to output a plurality of ADUs;

b) encryption means for encrypting the plurality of ADUs with different respective keys;

c) a communications network connected to the encryption means.

d) a customer terminal connected to the communications network and arranged to receive encrypted ADUs via the communications network;

e) a key generator programmed to generate a sequence of keys for use in decrypting ADUs:

f) decryption means connected to the key generator and arranged to decrypt the ADUs received at the customer terminal from the communications network; and

g) a store for storing a record of keys generated by the key generator means.

23. A customer terminal for use in a method according to claim 21, the customer terminal comprising:

a) a data interface for receiving data from a data communications medium;

b) a key generator programmed to generate a sequence of keys for use in decrypting ADUs:

c) decryption means connected to the data interface and to the key generator and arranged to decrypt ADUs received via the data interface;

d) a store containing a record of keys generated by the key generator; and

e) means for reading record data from the store and generating thereby a receipt for ADUs received and decrypted by the decryption means.

24. A method according to any one of claims 1 to 11 and 21, including generating keys from a seed value by iterated operations on the seed value by selected ones of a plurality of predetermined functions.

25. A method according to claim 24, in which the selection of the said predetermined functions is determined by the value of a ADU identity number.

26. A method according to 24 or 25 in which the predetermined functions are computationally symmetric.

27. A method according to claim 26 in which the said functions are left-shifted binary XOR and right-shifted binary XOR.

28. A method of operating a data communications system comprising:

a) at a remote data source, outputting a plurality of application data units (ADUs) ;

b) encrypting the ADUs;

c) communicating the ADUs to a plurality of customer terminals;

d) in the locality of each customer terminal, decrypting the ADUs; and

e) inducing a different characteristic variation in the value of the ADU's at different respective terminals.

29. A method according to claim 28, in which the characteristic variation is applied after decryption of the data.

30. A method according to claim 28, including generating a key for decryption of data at a respective customer terminal, which key includes a characteristic variation, and the said characteristic variation in the in the ADU data is induced by the characteristic variation in the key.

31. A method according to any one of claims 28 to 30 further comprising:

f) reading decrypted ADU data; and

g) determining from the characteristic variations in the ADU data the identity of a terminal at which the said data was originally received.

32. A method or system according to any one of the preceding claims, in which ADU's are communicated to a customer terminal via a communications network.

33. A method or system according to any one of the preceding claims, including a plurality of remote data sources, each outputting a respective plurality of ADU's.

34. A method of operating a data communications system comprising:

a) at a plurality of remote data sources, outputting a plurality of application data units (ADUs) ;

b) encrypting the ADUs from different remote data sources with different respective keys derived from a common seed value;

c) communicating the ADUs to a plurality of customer terminals;

d) in the locality of each customer terminal, decrypting the ADU's.

35. A method or system according to claim 33 or 34, in which the customer terminal receives a primary seed value common to different respective data streams from the plurality of data sources, and derives from the common primary key a plurality of different respective secondary seed values for decrypting ADU's from different respective data sources.

36. A method or system according to claim 35, in which data received from different data sources includes different respective source identity values, and the respective secondary seed value is generated from the primary seed value by modifying the primary seed value with the source identity value.

Figure 1

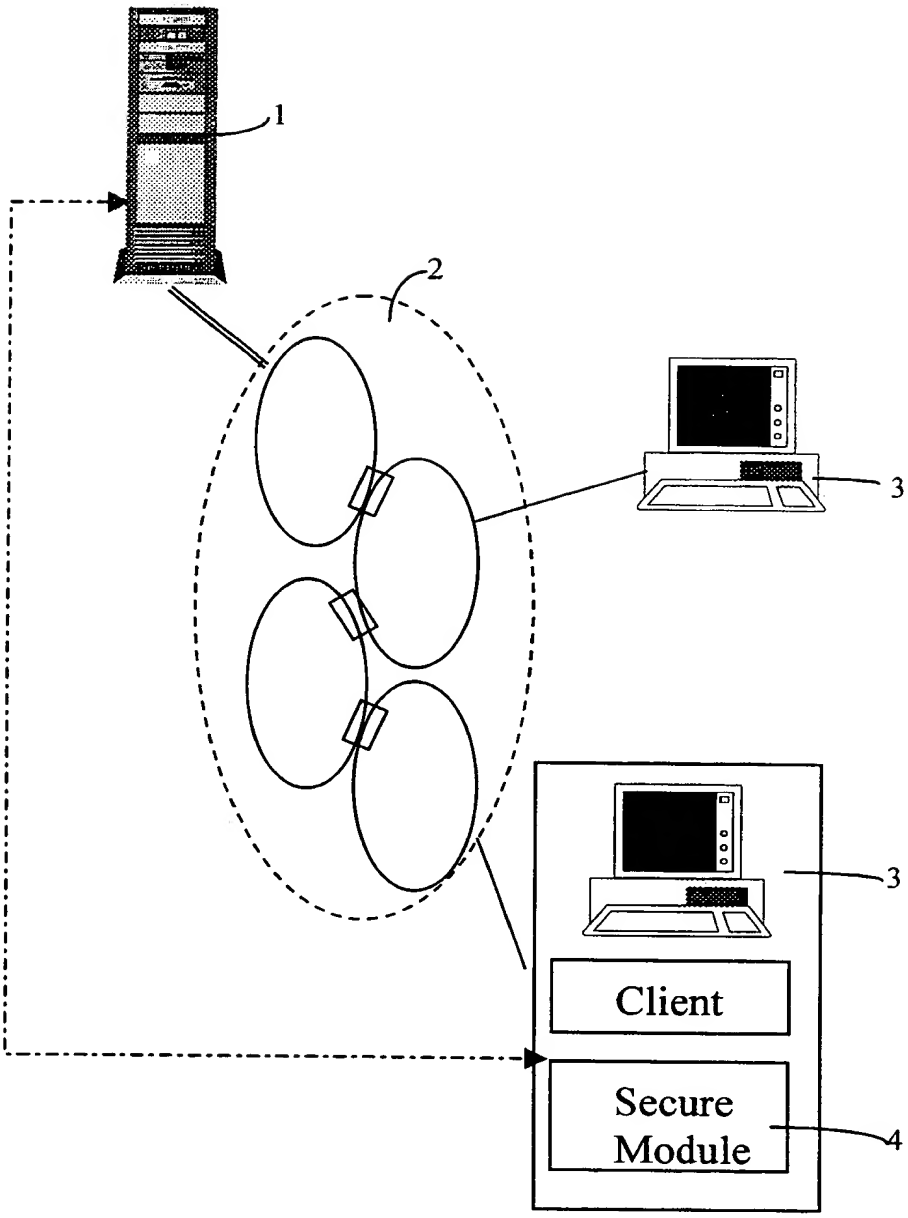


Figure 2

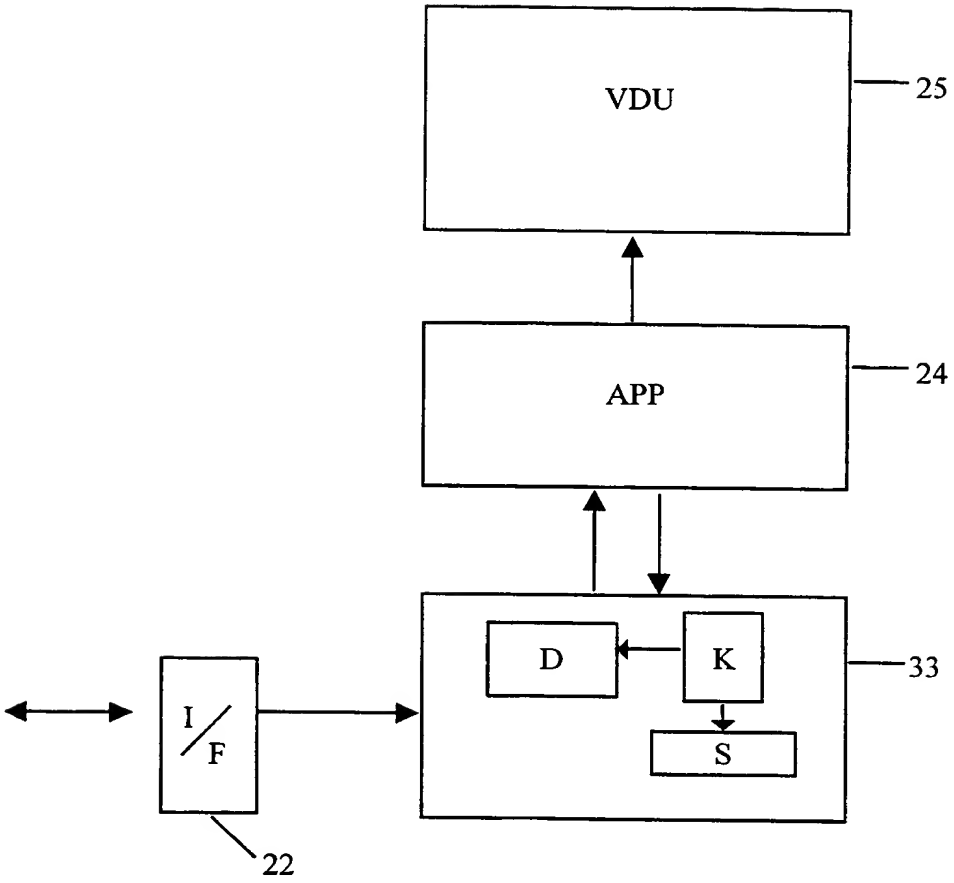


Figure 3

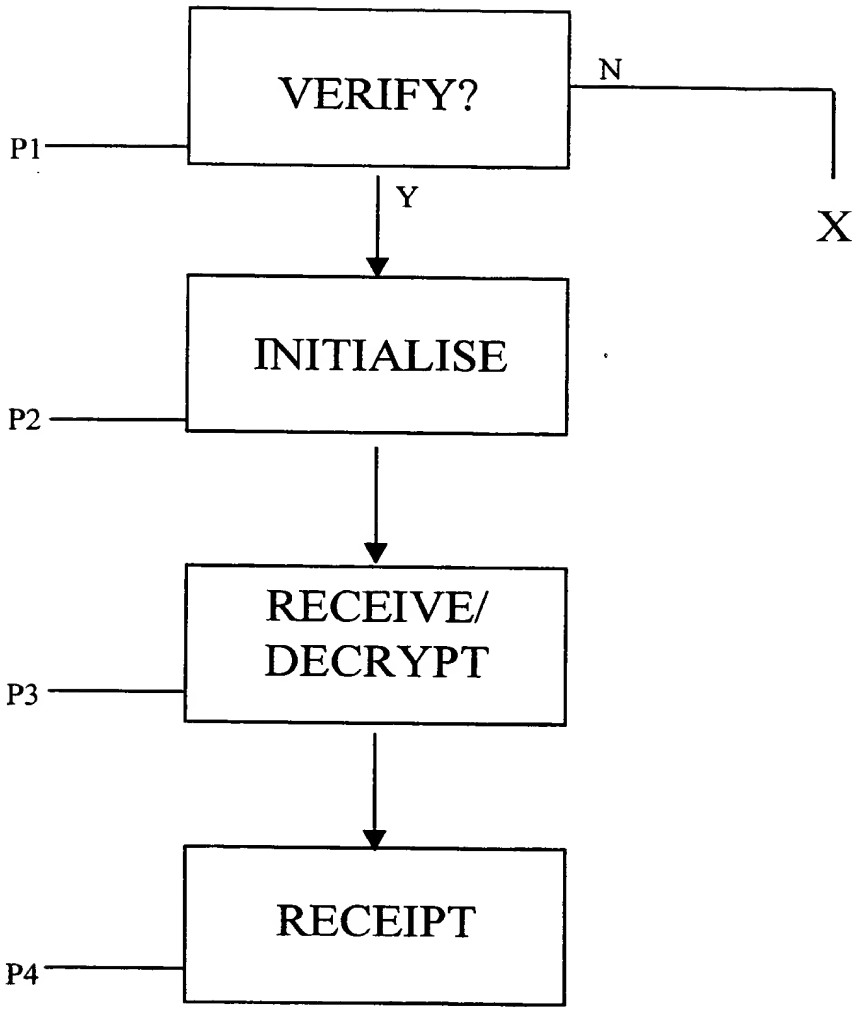


Figure 4

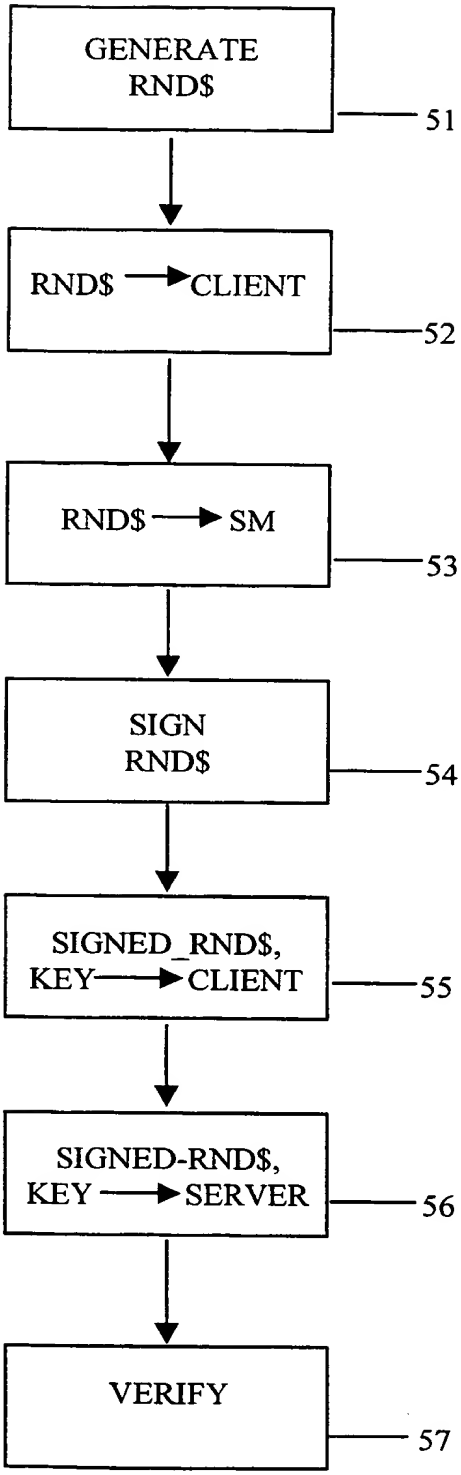

GENERATE RND$
51
RND$ → CLIENT
52
RND$ → SM
53
SIGN RND$
54
SIGNED_RND$, KEY → CLIENT
55
SIGNED-RND$, KEY → SERVER
56
VERIFY
57

Figure 5

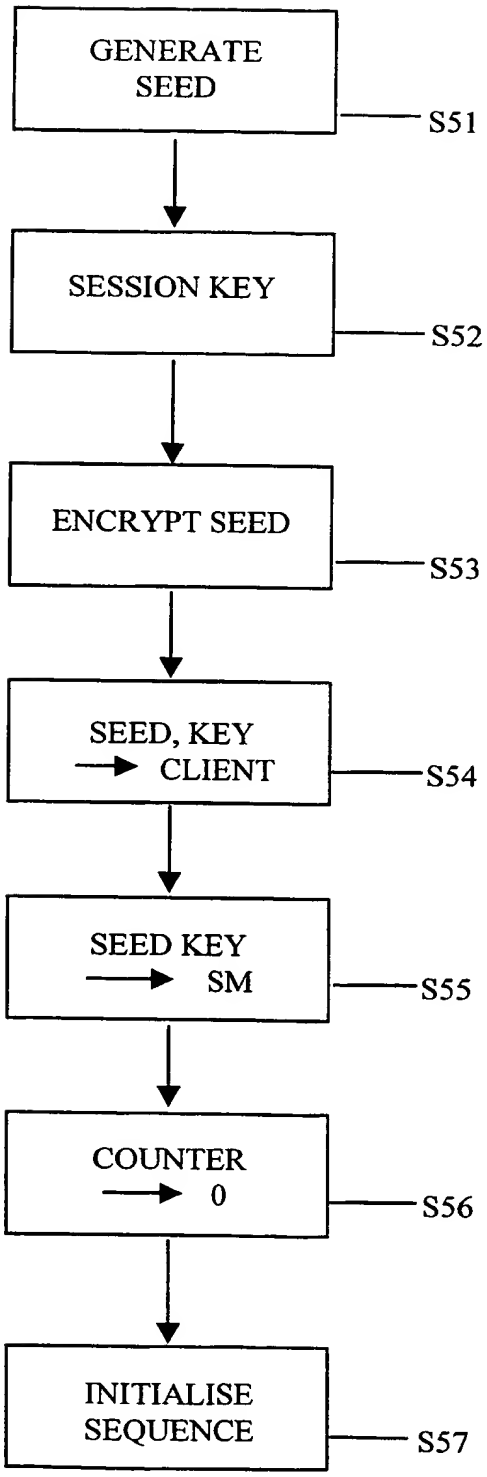

GENERATE SEED
S51
SESSION KEY
S52
ENCRYPT SEED
S53
SEED, KEY → CLIENT
S54
SEED KEY → SM
S55
COUNTER → 0
S56
INITIALISE SEQUENCE
S57

Figure 6

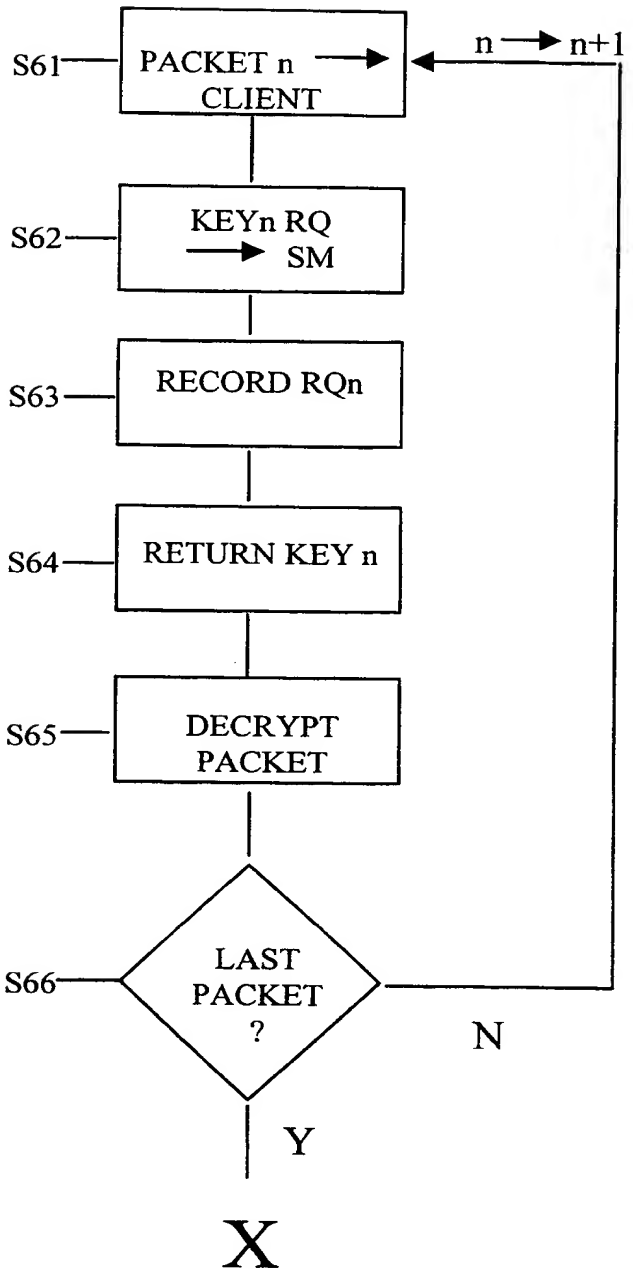

S61
PACKET n
CLIENT
n → n+1
S62
KEYn RQ
SM
S63
RECORD RQn
S64
RETURN KEY n
S65
DECRYPT
PACKET
S66
LAST
PACKET
?
N
Y
X

Figure 7

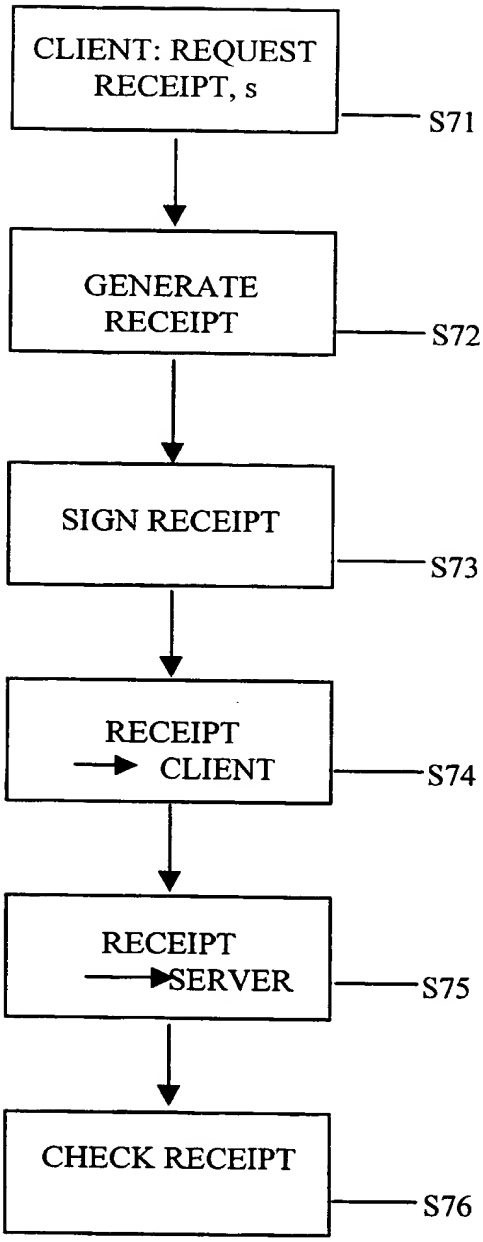

CLIENT: REQUEST RECEIPT, s
S71
GENERATE RECEIPT
S72
SIGN RECEIPT
S73
RECEIPT → CLIENT
S74
RECEIPT → SERVER
S75
CHECK RECEIPT
S76

Figure 8

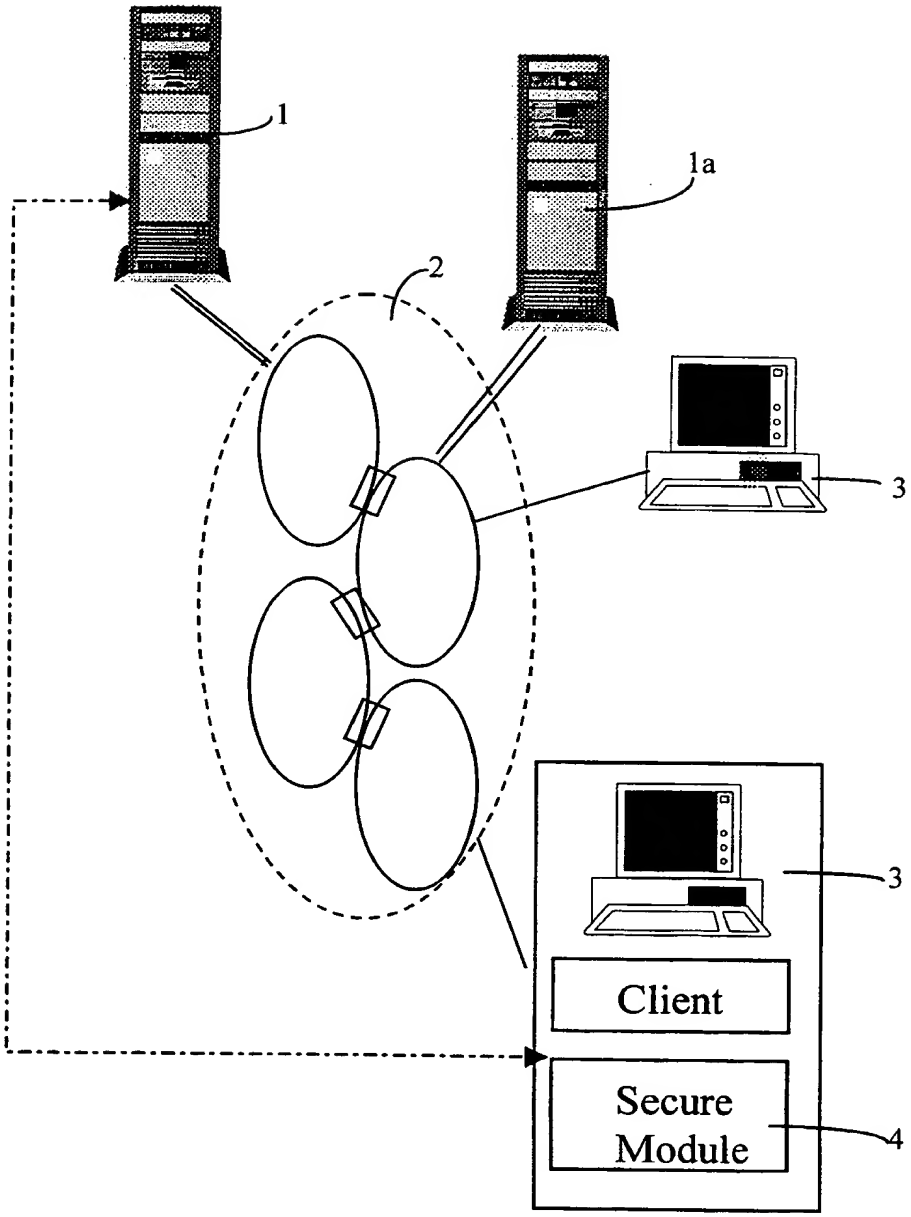
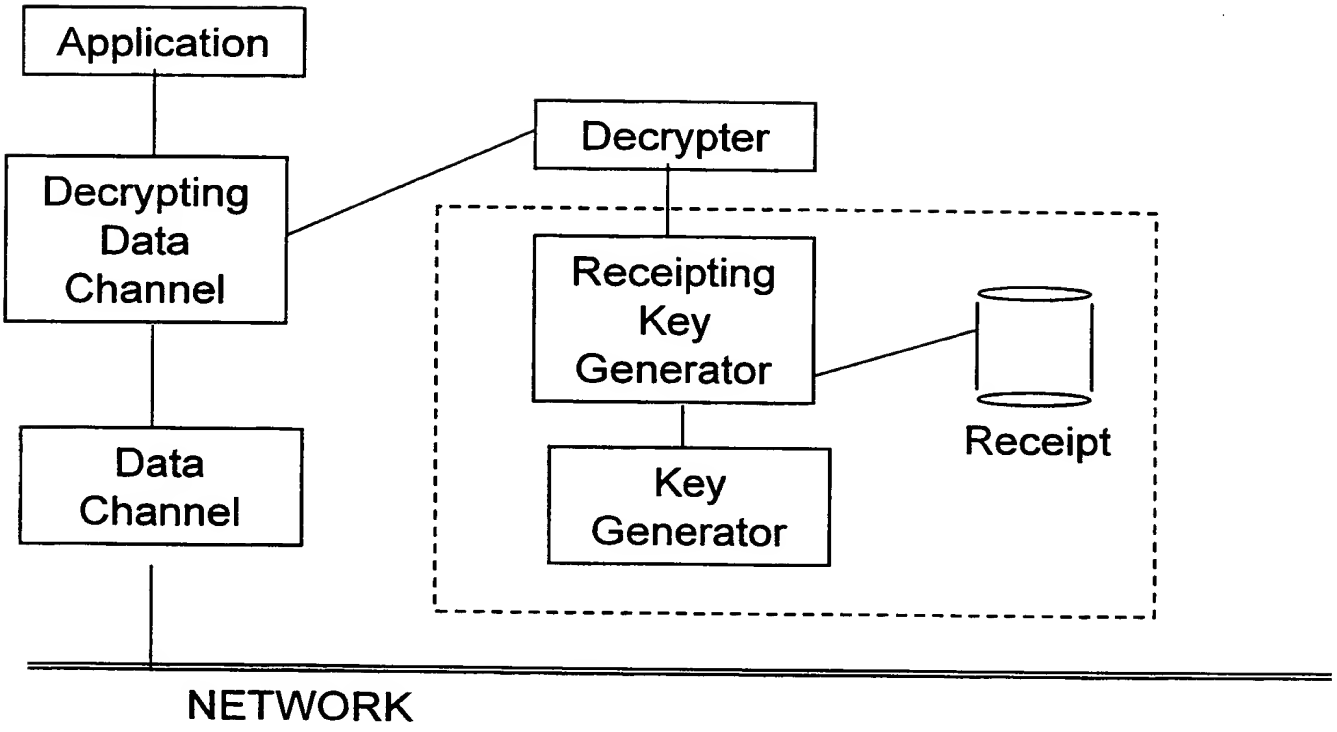


Figure 9


Application
Decrypting Data Channel
Data Channel
Decrypter
Receipting Key Generator
Key Generator
Receipt
NETWORK

INT[redacted]TIONAL SEARCH REPORT

[redacted]rnational Application No
PCT/GB 98/03755

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L12/14 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	POPP R ET AL: "SECURITY SERVICES FOR TELECOMMUNICATIONS USERS" BRINGING TELECOMMUNICATION SERVICES TO THE PEOPLE - ISS & N 1995, THIRD INTERNATIONAL CONFERENCE ON INTELLIGENCE IN BROADBAND SERVICE AND NETWORKS, HERAKLION, CRETE, OCT. 16 - 19, 1995. PROCEEDINGS, no. CONF. 3, 16 October 1995, pages 28-39, XP000593466 CLARKE A;CAMPOLARGO M; KARATZAS N (EDS) see abstract see page 30, line 7 - line 40 see page 34, line 13 - line 17	1-4,11, 17,18, 32-34
Y		12-15,28

	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 April 1999	15/04/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Poggio, F

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	BOTTURA G: "CHARGING AND TARIFFING FUNCTIONS AND CAPABILITIES FOR MANS" PROCEEDINGS OF THE NETWORK OPERATIONS AND MANAGEMENT SYMPOSIUM (NOM, MEMPHIS, APR. 6 - 9, 1992, vol. 1, 1 January 1992, pages 208-218, XP000344755 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS see page 210 - page 212 see page 214 - page 217 ---	12-15
Y	EP 0 534 419 A (IBM) 31 March 1993 see abstract see page 7, line 50 - page 11, line 52 see page 154, line 46 - page 155, line 21 see figures 10,12,15	28
A	---	7,20-36
A	WO 97 34426 A (ENCANTO NETWORK INC) 18 September 1997 see abstract see page 2, line 21 - page 3, line 32 see page 7, line 20 - page 10, line 30 ---	5-10,13, 16, 20-24,35
A	WO 93 09627 A (LEE ERNEST STEWART ;THOMPSON PHILIP MARTIN (CA)) 13 May 1993 see abstract see page 6, line 21 - line 28 see page 11, line 22 - line 25 see figure 1 ---	5,7,16, 20-24, 35,36
A	COFFEY T ET AL: "NON-REPUDIATION WITH MANDATORY PROOF OF RECEPT" COMPUTER COMMUNICATIONS REVIEW, vol. 26, no. 1, 1 January 1996, pages 6-17, XP000580016 see abstract see paragraph 3 - paragraph 4 see paragraph 7 -----	11,31,36

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/GB 98/03755

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0534419 A	31-03-1993	US 5200999 A	06-04-1993
		CA 2075329 A,C	28-03-1993
		JP 5216409 A	27-08-1993
		JP 8016826 B	21-02-1996
WO 9734426 A	18-09-1997	AU 1972597 A	01-10-1997
WO 9309627 A	13-05-1993	AU 2912692 A	07-06-1993
		CA 2123199 A	13-05-1993

17

PATENT COOPERATION TREATY

REC'D 23 MARS 2000
WIPO PCT

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
A25546 WO		
International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/GB98/03755	15/12/1998	19/12/1997
International Patent Classification (IPC) or national classification and IPC H04L12/14		
Applicant BRITISH TELECOMMUNICATIONS PUBLIC LIMITED.. et al.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 12 sheets, including this cover sheet.

   ☐ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☒ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations suporting such statement
   - VI ☐ Certain documents cited
   - VII ☒ Certain defects in the international application
   - VIII ☒ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
21/05/1999	20.03.00
Name and mailing address of the international preliminary examining authority: European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized officer Köppl, M Telephone No. +49 89 2399 8433

Form PCT/IPEA/409 (cover sheet) (January 1994)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/GB98/03755

I. Basis of the report

1. This report has been drawn on the basis of (*substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

Description, pages:

1-15 as originally filed

Claims, No.:

1-36 as originally filed

Drawings, sheets:

1/9-9/9 as originally filed

2. The amendments have resulted in the cancellation of:

☐ the description, pages:
☐ the claims, Nos.:
☐ the drawings, sheets:

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

4. Additional observations, if necessary:

IV. Lack of unity of invention

1. In response to the invitation to restrict or pay additional fees the applicant has:

☐ restricted the claims.

☐ paid additional fees.

☐ paid additional fees under protest.

☐ neither restricted nor paid additional fees.

2. ☒ This Authority found that the requirement of unity of invention is not complied and chose, according to Rule 68.1, not to invite the applicant to restrict or pay additional fees.

3. This Authority considers that the requirement of unity of invention in accordance with Rules 13.1, 13.2 and 13.3 is

   ☐ complied with.

   ☒ not complied with for the following reasons:

   see separate sheet

4. Consequently, the following parts of the international application were the subject of international preliminary examination in establishing this report:

   ☒ all parts.

   ☐ the parts relating to claims Nos. .

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-33
	No:	Claims	34-36
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-33
Industrial applicability (IA)	Yes:	Claims	1-36
	No:	Claims	

2. Citations and explanations

   see separate sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

see separate sheet

Re Item IV

Lack of unity of invention

The separate groups of inventions are:

Group I: claims 1 to 20, and 24 to 27 having as the special technical feature the steps of storing a record of the ADUs and generating a receipt for ADUs received;

Group II: claims 21 to 23 having as the special technical feature the step of generating a plurality of different keys and storing a record of the keys generated;

Group III: claims 28 to 33 having as the special technical feature the step of inducing a characteristic variation; and

Group IV: claims 34 to 36 having as the special technical feature the step of encrypting the ADUs with keys derived from a common seed value.

Due to differing special technical features, there exists no technical relationship among the groups of inventions I to IV. Since groups I to IV are not so linked so as to form a single general inventive concept, the application does not meet the requirement of unity of invention (see Rule 13.1 and 13.2 PCT).

Re Item V

Reasoned statement under Rule 66.2 (a) (ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1 Insofar as the present text can be understood given the observations on clarity as set out below Re Item VIII, the subject-matter of claims 34 to 36 is not novel in the sense of Article 33 (2) PCT and Rule 64.1 PCT, and the subject-matter of claims 1 to 33 does not involve an inventive step in the sense of Article 33 (3) PCT.

2 Reference is made to the following documents:

D1: COFFEY T ET AL: 'NON-REPUDIATION WITH MANDATORY PROOF OF RECEPT' COMPUTER COMMUNICATIONS REVIEW, vol. 26, no. 1, 1 January

1996, pages 6-17, XP000580016

D2: POPP R ET AL: 'SECURITY SERVICES FOR TELECOMMUNICATIONS USERS' BRINGING TELECOMMUNICATION SERVICES TO THE PEOPLE - ISS & N 1995, THIRD INTERNATIONAL CONFERENCE ON INTELLIGENCE IN BROADBAND SERVICE AND NETWORKS, HERAKLION, CRETE, OCT. 16 - 19, 1995. PROCEEDINGS, no. CONF. 3, 16 October 1995, pages 28-39, XP000593466 CLARKE A;CAMPOLARGO M; KARATZAS N (EDS)

D3: EP-A-0 534 419 (IBM) 31 March 1993

3 The subject-matter of claims 1, 12, and 17 is not based on an inventive step in the sense of Article 33 (3) PCT.

3.1 Document D1 discloses on page 7, section 1.1 "General Approach to the Non-Repudiation Problem" the features (a), (c), (e) and (f) of claim 1. Document D1 does not disclose the features (b) and (d) of claim 1 relating to encryption and decryption of data.

The objective problem underlying the present application is therefore to add authentication and confidentiality to the communication between the remote data source and the customer terminal while providing non-repudiation. This problem, however, is already solved as is disclosed in document D2 (see page 30, section 3 in the paragraph on user-to-user confidentiality, according to which data may optionally be encrypted in addition to authentication and non-repudiation of delivery).

Since both documents D1 and D2 lie in the same area of art as the instant application (see document D1, abstract, and document D2, page 29, chapter 2, third paragraph starting "Some network security features enable... correct billing ..."), it would have been obvious to a man skilled in the art to modify the solution of document D1 by applying the solution known from document D2 and thus arrive at the combination of features of claim 1. Therefore, the subject-matter of claim 1 appears to be obvious and consequently is considered not to involve an inventive step in the sense of Article 33 (3) PCT.

3.2 Claim 12 is a representation of method claim 1 in terms of system features. Therefore, the above arguments with respect to obviousness of claim 1 similarly apply to claim 12. Consequently, the subject-matter of claim 12 also is considered not to involve an inventive step in the sense of Article 33 (3) PCT.

3.3 Claim 17 largely recites the steps of method claim 1 in terms of apparatus features, the apparatus being part of the system as of claim 12. Therefore, the above arguments with respect to obviousness of claim 1 similarly apply to claim 17. Consequently, the subject-matter of claim 17 also is considered not to involve an inventive step in the sense of Article 33 (3) PCT.

4 Independent claims 21 to 23 differ from independent claims 1, 12, and 17 essentially in that a "plurality of keys" are utilized in the encryption process and that a "record of the keys" is stored for generating a receipt. However, these are only plain variations of what is already claimed in claims 1, 12, and 17 (particularly in view of document D3, see abstract thereof). Therefore, the above arguments with respect to obviousness of the subject-matter of claims 1, 12, and 17 similarly apply to claims 21 to 23. Therefore, the subject-matter of claims 21 to 23 also is considered not to involve an inventive step in the sense of Article 33 (3) PCT.

5 Document D3 discloses in figures 12 and 13 in conjunction with the associated description the features (a) to (d) of independent claim 28. By the applicant's own admission on page 4, lines 25 to 27 of the description, the feature (e) of claim 28 is well known in the art. It would have been obvious for a man skilled in the art to combine the teaching of document D3 with something that is well known in the art of cryptography. Therefore, the subject-matter of claim 28 is considered not to involve an inventive step in the sense of Article 33 (3) PCT on the basis of applicant's own admission.

6 Document D3 discloses in figures 12 and 13 in conjunction with the associated description the features (a) to (c) of independent claim 34. Moreover, document D3 discloses the feature (d) of claim 34 and the additional features of claims 35 and 36 (particularly see page 31, lines 40 to 46; and page 154, line 46 to page 155, line 21). Therefore, the subject-matter of claims 34 to 36 is considered not to be novel in the sense of Article 33 (2) PCT. At the very least, the subject-matter of

claims 34 to 36 is considered not to involve an inventive step in the sense of Article 33 (3) PCT.

7 None of the dependent claims 2 to 11, 13 to 16, 18 to 20, 24 to 27, and 29 to 33 appears to contain subject-matter which, when taken in combination with a respective independent claim, would lead to subject-matter which could be considered both to be novel and to involve an inventive step.

In particular, some of the dependent claims are a repetition of features already discussed above with respect to an unrelated independent claim. Additional features of other dependent claims are mere design options readily known to the person skilled in the art.

Therefore, the subject-matter of dependent claims 2 to 11, 13 to 16, 18 to 20, 24 to 27, and 29 to 33 is considered not to involve an inventive step in the sense of Article 33 (3) PCT.

Re Item VII

Certain defects in the international application

1 Independent claims 1, 12, 17, 21 to 23, 28, and 34 are not in the two-part form in accordance with Rule 6.3 (b) PCT, which in the present case would be appropriate, with those features known in combination from the prior art (document D1 or D2) being placed in a preamble (Rule 6.3 (b) (i) PCT) and with the remaining features being included in a characterising part (Rule 6.3 (b) (ii) PCT).

Independent claims 1, 12, 17, 21 to 23, 28, and 34 should therefore have been redrafted accordingly.

2 Reference signs in parentheses should have been inserted in all the claims to increase their intelligibility, Rule 6.2 (b) PCT. This applies to both the preamble and characterising portion (see also PCT International Preliminary Examination Guidelines III-4.11). Where a method claim makes reference to apparatus features, these should also have been accompanied by the respective reference signs wherever appropriate.

3 Contrary to the requirements of Rule 5.1 (a) (ii) PCT, the relevant background art disclosed in the documents D1 to D3 is not mentioned in the description, nor are these documents identified therein. The documents D1 to D3 should therefore have been mentioned in the introductory portion of the description (see also PCT International Preliminary Examination Guidelines II-4.4).

Re Item VIII
Certain observations on the international application

1 Although claims 1, 12, 17, 21 to 23, 28, and 34 have been drafted as separate independent claims, they appear to relate effectively to the same subject-matter and to differ from each other only with regard to the definition of the subject-matter for which protection is sought or in respect of the terminology used for the features of that subject-matter. The aforementioned claims therefore lack conciseness. Moreover, lack of clarity of the claims as a whole arises, since the plurality of independent claims makes it difficult, if not impossible, to determine the matter for which protection is sought, and places an undue burden on others seeking to establish the extent of the protection.

Hence, claims 1, 12, 17, 21 to 23, 28, and 34 do not meet the requirements of Article 6 PCT.

In order to overcome this objection, it would have been appropriate to file an amended set of claims defining the relevant subject-matter in terms of a minimum number of independent claims in each category (e. g. based on claims 1, 12, and 17) followed by dependent claims covering features which are merely optional (Rule 6.4 PCT).

2 Further observations on the claims:

2.1 Claims 1, 12 and 17 are not supported by the description, contrary to Article 6 PCT because the embodiments described in the description do not fall in their scope. Feature (e) of claim 1, feature (f) of claim 12, and feature (c) of claim 17 each calls for the storage or generation, respectively, of "a record of the ADUs". In the description on page 9, lines 27, and lines 32 to 33, it is stated, however, that

not "a record of the ADUs" is saved but rather "records of the request for a key". On page 9, line 34, it is stated that "a detailed record of receipt" is saved which also differs from the teaching of claims 1, 12, and 17. Moreover, it is stated on page 2, lines 21 to 22 that a "record is kept of the decryption of the ADUs" again differing from the teaching of claims 1, 12, and 17. Amendment of claims 1, 12, and 17 would have been required in order to remove this inconsistency between the claims and the description (see also PCT International Preliminary Examination Guidelines III- 4.3).

2.2 Claims 21 to 23 are not supported by the description, contrary to Article 6 PCT because the embodiments described in the description do not fall in their scope. Feature (e) of claim 21, feature (g) of claim 22, and feature (d) of claim 23 each calls for the storage of "a record of keys". In the description on page 9, lines 27, and lines 32 to 33, it is stated, however, that not "a record of the ADUs" is saved but rather "records of the request for a key". On page 9, line 34, it is stated that "a detailed record of receipt" is saved which also differs from the teaching of claims 21 to 23. Additionally, it is stated on page 2, lines 21 to 22 that a "record is kept of the decryption of the ADUs" which again does not clearly support the teaching of claims 21 to 23. Amendment of claims 21 to 23 would have been required in order to remove this inconsistency between the claims and the description (see also PCT International Preliminary Examination Guidelines III-4.3).

2.3 Claims 21, 22, and 28 to 36 are not clear because an apparently essential feature is missing. According to the description on page 1, lines 33 to 34 it is the object of the invention to determine the quality of service which has been delivered. Whereas in the description on page 9, line 32 to page 10, line 1 it is stated that a record of receipt is to be stored in order to solve this problem, claims 28 to 36 do not have a corresponding feature that would address the object of the invention. Consequently, claims 28 to 36 apparently lack an essential feature and thus are not clear in the sense of Article 6 PCT (see also PCT International Preliminary Examination Guidelines III-4.3).

2.4 Claims 1, 11, 12, 17, and 23 are not clear in the sense of Article 6 PCT because they introduce the term "receipt" which does not have a generally accepted technical meaning. It is required that the term be further defined by its intended

technical meaning as defined in this application. In this regard, a "receipt" appears to have a specific relation to the meaning of the terms "record of the ADUs" and "record of keys", respectively. Clarification would have been required, e. g. on the basis of the description on page 7, lines 22 to 26 (see also PCT International Preliminary Examination Guidelines III-4.2).

2.5 The term "different" used in claims 5, 7, 8, 16, 21, 22, 28, an 34 to 36 renders these claims unclear in the sense of Article 6 PCT because it tries to define subject-matter in terms of negative features (teaching of what not to do; here "different" means "do not do the same") instead of providing a definition of the invention on the basis of positive features (teaching of what to do). However, a negative definition of the invention should only be made in exceptional circumstances as outlined in PCT International Preliminary Examination Guidelines III-4.12. The claims should have been amended so as to avoid negative features (e. g. as used in claim 23, feature (b)).

2.6 The term "outside" used in claim 3 renders the claim unclear in the sense of Article 6 PCT because it tries to define subject-matter in terms of negative features (teaching of what not to do; here "outside" means "do not put in the secure module") instead of providing a definition of the invention on the basis of positive features (teaching of what to do). However, a negative definition of the invention should only be made in exceptional circumstances as outlined in PCT International Preliminary Examination Guidelines III-4.12. Claim 3 should have been amended so as to avoid negative features.

2.7 Claims 32 and 33 and not clear because they try to designate in one claim both a method and a system which renders these claims obscure (see also PCT International Preliminary Examination Guidelines III-4.1).

3 Observations on the description:

3.1 In the description on page 6, line 25, reference is made to the drawings by reference signs 2a-2d. However, these reference signs do not appear in any of the figures (see also PCT International Preliminary Examination Guidelines II-4.8).

3.2 In the description on page 8, lines 1 to 12, reference is made to the drawings by reference sign 23. However, these reference signs do not appear in any of the figures (figure 2 has only reference sign 33). Correction would have been required (see also PCT International Preliminary Examination Guidelines II-4.8).

3.3 In the description, the passage on page 10, lines 28 to 30 is grammatically incorrect such that it is hardly possible to understand the technical sense (see also PCT International Preliminary Examination Guidelines II-4.1 (ii)).

3.4 On page 11, lines 8 to 11, citation is made of a document by an internet address only. The document should additionally have been cited by regular bibliographic data (particularly publication date and location as well as the publisher) or the citation should be deleted.

3.5 On page 13, lines 30 to 34, citation is made of a document not using its publication number. The citation should therefore be replaced by the document's publication number, which presumably is WO 99/33242. Since the disclosure of this document is not essential to satisfy the requirements of Article 5 PCT, the sentence on page 13, lines 32 and 33 "The contents ..." is obviously unnecessary and should have been deleted (Rule 9.1 (iv) PCT; see also PCT International Preliminary Examination Guidelines II-4.17).

Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference E4351-00	**FOR FURTHER ACTION**	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/JP98/05462	International filing date (*day/month/year*) 03 December 1998 (03.12.98)	Priority date (*day/month/year*) 04 December 1997 (04.12.97)
International Patent Classification (IPC) or national classification and IPC C08B 15/08		
Applicant ASAHI KASEI KOGYO KABUSHIKI KAISHA		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 3 sheets, including this cover sheet.

☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of _____ sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand 06 January 1999 (06.01.99)	Date of completion of this report 08 December 1999 (08.12.1999)
Name and mailing address of the IPEA/JP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/JP98/05462

I. Basis of the report

1. With regard to the **elements** of the international application:*

☒ the international application as originally filed

☐ the description:

pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

☐ the claims:

pages _____, as originally filed
pages _____, as amended (together with any statement under Article 19
pages _____, filed with the demand
pages _____, filed with the letter of _____

☐ the drawings:

pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

☐ the sequence listing part of the description:

pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).

☐ the language of publication of the international application (under Rule 48.3(b)).

☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

☐ contained in the international application in written form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* *Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).*

** *Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-25	YES
	Claims		NO
Inventive step (IS)	Claims	1-25	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-25	YES
	Claims		NO

2. Citations and explanations

The subject matters of claims 1-25 are neither described in any of the documents cited in the ISR nor obvious to a person skilled in the art.

FS

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	FOR FURTHER ACTION	see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.
A25546 WO		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/GB 98/ 03755	15/12/1998	19/12/1997

Applicant

BRITISH TELECOMMUNICATIONS PUBLIC LIMITED.. et al.

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 3 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

   a. With regard to the **language,** the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

   [ ] the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

   b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing :

   [ ] contained in the international application in written form.

   [ ] filed together with the international application in computer readable form.

   [ ] furnished subsequently to this Authority in written form.

   [ ] furnished subsequently to this Authority in computer readble form.

   [ ] the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

   [ ] the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

2. [ ] **Certain claims were found unsearchable** (See Box I).

3. [ ] **Unity of invention is lacking** (see Box II).

4. With regard to the **title,**

   [X] the text is approved as submitted by the applicant.

   [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**

   [X] the text is approved as submitted by the applicant.

   [ ] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is Figure No. 1

   [X] as suggested by the applicant.

   [ ] because the applicant failed to suggest a figure.

   [ ] because this figure better characterizes the invention.

   [ ] None of the figures.

INTERNATIONAL SEARCH REPORT

[redacted] International Application No
[redacted] GB 98/03755

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L12/14 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	POPP R ET AL: "SECURITY SERVICES FOR TELECOMMUNICATIONS USERS" BRINGING TELECOMMUNICATION SERVICES TO THE PEOPLE - ISS & N 1995, THIRD INTERNATIONAL CONFERENCE ON INTELLIGENCE IN BROADBAND SERVICE AND NETWORKS, HERAKLION, CRETE, OCT. 16 - 19, 1995. PROCEEDINGS, no. CONF. 3, 16 October 1995, pages 28-39, XP000593466 CLARKE A;CAMPOLARGO M; KARATZAS N (EDS) see abstract see page 30, line 7 - line 40 see page 34, line 13 - line 17	1-4,11, 17,18, 32-34
Y	--- -/--	12-15,28

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 April 1999	15/04/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Poggio, F

1

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category.°	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	BOTTURA G: "CHARGING AND TARIFFING FUNCTIONS AND CAPABILITIES FOR MANS" PROCEEDINGS OF THE NETWORK OPERATIONS AND MANAGEMENT SYMPOSIUM (NOM, MEMPHIS, APR. 6 - 9, 1992, vol. 1, 1 January 1992, pages 208-218, XP000344755 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS see page 210 - page 212 see page 214 - page 217	12-15
Y	EP 0 534 419 A (IBM) 31 March 1993 see abstract see page 7, line 50 - page 11, line 52 see page 154, line 46 - page 155, line 21 see figures 10,12,15	28
A		7,20-36
A	WO 97 34426 A (ENCANTO NETWORK INC) 18 September 1997 see abstract see page 2, line 21 - page 3, line 32 see page 7, line 20 - page 10, line 30	5-10,13, 16, 20-24,35
A	WO 93 09627 A (LEE ERNEST STEWART ;THOMPSON PHILIP MARTIN (CA)) 13 May 1993 see abstract see page 6, line 21 - line 28 see page 11, line 22 - line 25 see figure 1	5,7,16, 20-24, 35,36
A	COFFEY T ET AL: "NON-REPUDIATION WITH MANDATORY PROOF OF RECEPT" COMPUTER COMMUNICATIONS REVIEW, vol. 26, no. 1, 1 January 1996, pages 6-17, XP000580016 see abstract see paragraph 3 - paragraph 4 see paragraph 7	11,31,36

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/GB 98/03755

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0534419 A	31-03-1993	US 5200999 A	06-04-1993
		CA 2075329 A,C	28-03-1993
		JP 5216409 A	27-08-1993
		JP 8016826 B	21-02-1996
WO 9734426 A	18-09-1997	AU 1972597 A	01-10-1997
WO 9309627 A	13-05-1993	AU 2912692 A	07-06-1993
		CA 2123199 A	13-05-1993